UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/854,251	05/11/2001	Sarver Patel	18	7868

7590 09/20/2005

Docket Administrator (Room 3C-512)
Lucent Technologies Inc.,
600 Mountain Avenue
P.O. Box 636
Murray Hill, NJ 07974-0636

EXAMINER	
FIELDS, COURTNEY D	
ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 09/20/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/854,251	PATEL, SARVER	
	Examiner	Art Unit	
	Courtney D. Fields	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 July 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,7-11,14,16 and 19-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,7-11,14,16 and 19-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 5-6,12-13,15, and 17-18 have been cancelled.

2. Claims 1,7,14 and 16 have been amended.

3. Claims 19-21 have been added.

4. Claims 1-4,7-11,14,16, and 19-21 are pending.

Response to Arguments

5. Applicant's arguments filed 07 July 2005 have been fully considered but they are not persuasive.

6. Referring to the rejection of claims 1 and 14, the Applicant contends and argues that the prior art (Bellare et al.) does not teach nor suggest any MAC-generation method in which the compression function is called only once. The Examiner respectfully disagrees and asserts that Bellare et al. teaches performing a compression function only once will prevent extra computation of the key k which is generated or shared the first time and then stored upon the function of NMAC. (See pages 14-15)

Referring to the rejection of claims 1 and 14, the Applicant contends and argues that the prior art (Bellare et al.) does not teach nor suggest an input message being processed by a hash function nested within a keyed hash function. The Examiner respectfully disagrees and asserts that Bellare et al. does teach an input message being processing by a hash function nested within a keyed hash function as disclosed in the functionality of a NMAC (nested message authentication code). The hash function F is keyed with a secret key k_2 and the message x is hashed to the output of $Fk_2(x)$. The

output $Fk_2(x)$ is padded according to block size and the result of $Fk_2(x)$ is keyed with a secret key k_1, and is hashed with an outer hash function F. (See pages 9-11)

Referring to the rejection of claims 1 and 14, the Applicant contends and argues that the prior art (Bellare et al.) does not teach nor suggest any function for MAC generation that has two branches, leading to different types of processing, depending on determination of whether the input message fits within a block. The Examiner respectfully disagrees and asserts that in response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., any function for MAC generation that has two branches, leading to different types of processing) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Referring to the rejection of claims 7 and 16, the Applicant contends and argues that the prior art (Bellare et al.) does not teach nor suggest any hash function or MAC-generating function in which two portions of an input message are processed differently, and then concatenated, and the concatenation used as input for further processing. The Examiner respectfully disagrees and asserts that Bellare et al. does teach a keyed hash function of two portions k and x of an input message. The concatenation of k and x can be processed differently by hashing data x using key k or iterating hash functions using a fixed and known IV. (See page 8)

7. Therefore, the rejection of claims 1-4,7-11,14,16, and 19-21 are maintained in view of the reasons above and in view of the reasons below.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-4,7-11,14,16, and 19-21 are rejected under 35 U.S.C. 102(b) as being anticipated by Bellare et al. (Keying Hash Function for Message Authentication).

Referring to the rejection of claims 1 and 14, Bellare et al. discloses a method of processing a message for authentication comprising:

determining whether the message fits within an input block of a compression function (See page 7)

performing a single iteration of the compression function using a key and the message as inputs when the message fits within an input block of the compression function and using a result from the compression function without further iteration thereof to produce a message authentication code (See pages 9-10 and page16)

and using a hash function nested within a keyed hash function to process the message when the message does not fit within an input block of the compression function and using a result from the keyed hash function to produce a message authentication code (See pages 6-7 and page 10)

As per claims 2,7,and 16, Bellare et al. discloses a method comprising the steps of: providing a first portion and a second portion of the message, performing a hash function using the first portion as an input to achieve a result, and performing a keyed hash function using a concatenation of the second portion and the result as inputs (See pages 7-9,13, and 15-16)

As per claims 3 and 10, Bellare et al. discloses the claimed limitation wherein the hash function is an iterated hash function F and the keyed hash function is a keyed compression function F (See pages 7-9)

As per claims 4 and 11, Bellare et al. discloses the claimed limitation wherein the hash function is an iterated hash function F and the keyed hash function is an iterated hash function F (See pages 7-9)

As per claim 8, Bellare et al. discloses the claimed limitation wherein determining whether the message fits within an input block of a compression function and performing the steps of providing, performing, and performing when the message does not fit within an input block of the compression function (See pages 6-7 and page 10)

As per claim 9 Bellare et al. discloses a method comprising the steps of: determining whether the message fits within an input block of a compression function and performing a single iteration of a compression function using a key and the message as inputs when the message fits within an input block of the compression function (See page 15, Section 6)

Referring to the rejection of claim 19, Bellare et al. discloses a method of processing a message x for authentication comprising:

(a) conditionally processing x to provide an intermediate result y, (See page 10)

(b) compressing x or y with a keyed compression function having a block size (See page 11)

(c) and providing a result of the compressing step for use in a message authentication scheme, wherein (a) comprises using a hash function to compress at least a portion of x and is carried out on condition that x exceeds the block size (See page 11)

As per claim 20, Bellare et al. discloses the claimed limitation wherein (a) comprises providing a first portion and a second portion of the message x, performing a hash function using the first portion as an input to achieve a result, and concatenating the result with the second portion (See pages 7-9)

Referring to the rejection of claim 21, Bellare et al. discloses a message authentication system comprising:

processing circuitry configured to determine whether a message x is larger than an input block size b of a keyed compression function (See pages 9-10)

processing circuitry configured to apply a hash function to compress at least a portion of x, thereby to provide an intermediate result y, the processing circuitry to be activated only in the event that x is larger than b (See page 10)

and processing circuitry configured to compress x or y with the keyed compression function, thereby to provide a result for use in a message authentication scheme (See page 11)

Conclusion

3. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Courtney D. Fields whose telephone number is 571-272-3871. The examiner can normally be reached on Mon - Thurs. 6:00 - 4:00 pm; off every Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

cdf
September 12, 2005

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER